Development Security Procedures

During the development life cycle, there are security milestones that will be outlined in this document. It is required that all developers follow these security requirements during development and throughout the application life span.

During Development

1. When estimating time/cost for a proposed project, approximately 40 hours will be added to all estimates to allow for security testing.

2. The first security scan will be performed on development when the major functionality of the project is completed. This will be at the discretion of the developer and may be repeated if there are several major components. After each of these security scans, the developer will be responsible for addressing any issues found and repairing these issues. When reparations are complete, the developer will request another scan to assure all issues have been repaired.

3. The next security scan will be performed when the application is complete on development and ready for transfer to user testing phase. Again, this testing will be performed by the individuals listed above. After each of these security scans, the developer will be responsible for addressing any issues found and repairing these issues. When reparations are complete, the developer will request another scan to assure all issues have been repaired. Load testing may also be performed at this time.

4. When the application is fully tested and has passed security testing with Cenzic Hailstorm in the test environment, security approval will be requested.

5. Upon approval, the developer will then forward this approval to the web team and request PCI scanning.

6. Only after all of the above requirements are met, the application will then be moved into production.

7. **Application Life Span in Production**
    - All applications in production should be rescanned with Cenzic Hailstorm every 6 months and the results of the current scan saved to a common location.

- Developers should be aware that their applications are subject to additional security scans at any time with other security tools or tools used by hackers. These additional tests will be performed by the security group and the web administrators.

- Anytime a major change is made to the application, the application must be rescanned with Cenzic Hailstorm and reapproved by the security group. Major changes are: the addition of any new inputs, the addition of database functionality, changes in the current inputs, or changes in the current database functionality. These changes will be made and tested on the development server.

- Developers will also be aware of the age of the applications. Since older code is more susceptible to hacking, older applications should be scanned more frequently than newer applications.